IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 1, June 2023

Secure Data Storage System and Data Leakage Detection

Prof. Rupali Jadhav, Mr. Tejas Rahane, Mr. Chaitanya Shelar, Suyash Shelar, Mr. Abhijeet Waghmode,

Department of Computer Science

Zeal College of Engineering Research, Pune, India

Abstract*: Given the size and rate of growth of these networks, data carried across them must be secure and confidential. A vital resource for data storage is cloud servers. Cloud servers therefore need to be secured and cannot be left vulnerable to the possibility of being used by hackers for theft or exposure. To ensure the security and privacy of the data, they need strategic plans. The proposed system employs three strategies to ensure data security. The plans call for data encryption, distribution over many clouds, and authentication of data sharing using just a secret key. The system is initially configured to provide data sharing over a secure channel using the Lightweight technique of encryption. Then, to prevent any loss, data is copied between clouds and scattered using the DROP technique throughout many clusters. Access to certain data segments can only be explicitly granted by a third private key to those who require the information. A trapdoor that detects any unethical requests for data sharing stops the requests and identifies the person in charge of any data leak*s.

Keywords: Energy efficient algorithm, Manets, total transmission energy, maximum number of hop, network lifetime

REFERENCES

[1] Y. Kao, K. Huang, H. Gu and S. Yuan, "UCloud: A usercentric key management scheme for cloud data protection", IET Inf. Secur., vol. 7, no. 2, pp. 144-154, Jun. 2013.

[2] A. Al-Haj, G. Abandah and N. Hussein, "Crypto-based algorithms for secured medical image transmission", IET Inf. Secur., vol. 9, no. 6, pp. 365-373,Nov.2015.

[3] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, et al., "A secure and efficient ciphertext-policy attributebased proxy re-encryption for cloud data sharing", Future Generat. Comput. Syst., vol. 52, pp. 95-108, Nov. 2015.

[4] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing", IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1265-1277, Jun. 2016.

[5] H. Liu, X. Li, M. Xu, R. Mo and J. Ma, "A fair data access control towards rational users in cloud storage", Inf. Sci., vol. 418, pp. 258-271, Dec. 2017.

[6] Z. Liu, Z. L. Jiang, X. Wang and S. M. Yiu, "Practical attribute-based encryption: Outsourcing decryption attribute revocation and policy updating", J. Netw. Comput. Appl., vol. 108, pp. 112-123, Apr. 2018.

[7] R. Li, C. Shen, H. He, X. Gu, Z. Xu and C.-Z. Xu, "A lightweight secure data sharing scheme for mobile cloud computing", IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344- 357, Apr. 2018.

[8] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, et al., "An efficient attribute-based encryption scheme with policy update and file update in cloud computing", IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6500-6509, Dec. 2019.

[9] E. Zaghloul, K. Zhou and J. Ren, "P-MOD: Secure privilegebased multilevel organizational data-sharing in cloud computing", IEEE Trans. Big Data, vol. 6, no. 4, pp. 804-815, Dec. 2020

DOI: 10.48175/568

ISSN 2581-9429 IJARSCT